1

SYSTEM, DEVICE, AND METHOD FOR COMMUNICATING USER IDENTIFICATION INFORMATION OVER A COMMUNICATIONS NETWORK

TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to information transfer over a network and more particularly to a system, device, and method for communicating user
5   identification information over a communications network.

BACKGROUND OF THE INVENTION

Network interfaces known as Service Selection Gateways (SSGs) or Network Access Servers (NASs) terminate Layer 2 protocol connections from network users. Layer 2, or Data Link, information regards the procedures and protocols used to operate communications lines and may include information about network links such as bandwidth, latency, and utilization. The user connections may be of various types, including traditional Point-to-Point Protocol (PPP) over a dial-up connection, Point-to-Point Protocol over Ethernet (PPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (ATM) (PPPoA), Point-to-Point Protocol over Ethernet over Ethernet (PPPoEoE), or other Layer 2 protocols such as GPRS Tunneling Protocol (GTP) that terminate in General Packet Radio Service (GPRS) nodes. In the traditional setting the SSGs handle user authentication and user Internet Protocol (IP) address assignment when a user logs on by using a RADIUS or other Authentication, Authorization, and Accounting (AAA) server. The SSG associates a user-ID with the IP address of that user and retains the user-ID - IP address mapping until the user logs off the network. When the user logs off the network, an "Accounting Stop" message is communicated to the AAA server, and the IP address is returned to an address pool of available addresses.

Network Service Providers (SPs) may locate some client-specific services at the edge of the network in a Point of Presence (POP) location. This enables client-specific services such as data content rating and filtering to be enabled and enforced as closely as possible to the client devices. A network interface,

hereinafter referred to as a Client Services Gateway (CSG), exists "upstream" from the NAS within the POP and is operable to provide these types of client services. In order to provide client specific services in a POP, the CSG needs to associate a user-ID with a given client address in order to retrieve the user profile that specifies the services to be applied to a user request. Therefore, it is desirable to have a CSG recognize which incoming packets are associated with a given service.

SUMMARY OF THE INVENTION

From the foregoing, it may be appreciated by those skilled in the art that a need has arisen for a technique to provide client services closer to the location of users in a network. In accordance with the present invention, a system, device, and method for communicating user identification information in a communications network are provided that substantially eliminate or greatly reduce disadvantages and problems associated with conventional information transfer and processing techniques in a network.

According to an embodiment of the present invention, there is provided a system for exchanging user identification information over a communications network that includes a first network interface establishing a communications session with a network user. The network user has a network locator address within the network. A second network interface processes requests from the network user received during the communications session. The second network interface unit determines whether it has stored within its local memory an identity of the network user associated with the network locator address. If the identity of the network user is stored in the local memory for the network locator address, the second network interface obtains additional information associated with the network user. The second network interface then processes the request according to the additional information. If the identity of the network user is not stored in the local memory, the second network interface unit sends a query to the first network interface unit. The first network interface obtains the identity of the network user in response to the query for

forwarding to the second network interface. The second network interface stores the identity of the network user in the local memory and associates it with the network locator address of the request. The second network interface can then obtain the additional information associated with the network user and process the request accordingly.

The present invention provides various technical advantages over conventional information transfer and processing techniques in a network. For example, one technical advantage is requiring only a single "sign on" from a network user, thus eliminating multiple challenges to provide a user-ID and password. Another technical advantage is to allow for multiple CSGs in the event that the SSG routes information requests to different CSGs. Yet another technical advantage is to allow "upstream" CSGs to unambiguously determine the user-ID for each network user IP address. Other technical advantages may be readily ascertainable by those skilled in the art from the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like reference numerals represent like parts, in which:

FIGURE 1 illustrates a simplified diagram of a communications network environment;

FIGURE 2 illustrates a simplified scheme of a Client Services Gateway (CSG) in the communications network environment, including data exchanges that will take place during a typical user login;

FIGURE 3 illustrates a simplified scheme of Client Services Gateways (CSGs) in the communications network environment, including data exchanges that will take place during which the user changes Internet Protocol (IP) addresses; and

FIGURE 4 illustrates a simplified scheme of the Client Services Gateway (CSG) in the communications network environment, including data exchanges that will take place during a typical user login.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 shows a simplified diagram of a communications network environment 100. Network 100 includes a user 102 connected by a data connection 110 to a Service Provider (SP) at the Point of Presence (POP) 140. Data connection 110 may be a traditional Point-to-Point Protocol (PPP) over a dial-up connection, Point-to-Point Protocol over Ethernet (PPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (ATM) (PPoA), Point-to-Point Protocol over Ethernet over Ethernet (PPPoEoE), or other Layer 2 protocols such as GPRS Tunneling Protocol (GTP) that terminate in General Packet Radio Service (GPRS) nodes. POP 140 may be a physical location where the SP receives data requests from user 102 and network equipment is present and operable to permit user 102 to communicate over network 100. An additional user 104 is also illustrated and is shown connected to POP 140 by data connection 112, which may be of any of the same communication formats as data connection 110.

The SP POP 140 contains a network interface known as a Network Access Server (NAS) 120 and hereinafter referred to as a Service Selection Gateway (SSG) 120. SSG 120 terminates Layer 2 protocol connections from user 102. One task typically performed by SSG 120 is identification of user 102 by verifying the user-ID and password provided by user 102. An additional task performed by SSG 120 is to assign an Internet Protocol (IP) address to user 102 when user 102 seeks to initiate communication on network 100. The SSG 120 is operable to retain user-ID and IP address information in memory until the user 102 terminates the communication.

8

An SP may move some user-specific services to the edge of the network 100 at POP 140 so that user-specific policies, such as data content rating and filtering, may be enabled and enforced as close as possible to user 102. A second network interface, hereinafter referred to as a Client Service Gateway (CSG) 130, exists "upstream" from the SSG 120 within the POP 140. In a communication network setting, an "upstream" interface is one in which data from a "downstream" interface passes on its way to or from the network 150 and servers 160. CSG 130 has stored in its memory or otherwise has access to a plurality of user-IDs and the services that are to be applied to an individual user-ID. CSG 130 is operable to associate a user-ID with a user IP address so that CSG 130 can retrieve the user profile stored in its memory that specifies the services to be applied as well as recognize which incoming data packets are associated with a request of a specific user 102.

FIGURE 2 shows a simplified scheme of a CSG 130 in the communications network environment 100 including data communications that will take place during a login by user 102. Preferably a many-to-many relationship exists between the SSGs 120 and CSGs 130, wherein a CSG 130 may receive data traffic from a plurality of SSGs 120 and/or a SSG 120 may route data to a plurality of CSGs 130. Any given data flow, however, arrives at a specific CSG 130 from a specific SSG 120.

An exemplary login sequence by user 102 is initiated by user 102 opening a data session with SSG 120. In a preferred embodiment of the present invention, the data session is a Point-to-Point Protocol (PPP) over a dial-up connection, or other form of communication such as Point-

to-Point Protocol over Ethernet (PPoE), Point-to-Point over Asynchronous Transfer Mode (ATM) (PPoA), Point-to-Point Protocol over Ethernet over Ethernet (PPPoEoE), or GPRS Tunneling Protocol (GTP). Upon initiating the data session, user 102 sends a user-ID and password to SSG 120 for authentication as is shown in communication 210. SSG 120 responds to communication 210 from user 102 by querying an authentication server 240 with the user-ID and password of user 102 as is shown in communication 212. In a preferred embodiment of the present invention, authentication server 240 is a RADIUS authentication or other form of Authentication, Authorization, and Accounting (AAA) server 240. If the user-ID and password match what is stored in the memory of authentication server 240, authentication server 240 communicates that information to SSG 120 as shown in communication 214.

After SSG 120 has authenticated the user-ID and password, user 102 opens a data communication session at communication 216 SSG 120 establishes a link for the session to its portal, Service Selection Dashboard (SSD) 250 at communication 218. The session may be in any data format, but in a preferred embodiment of the present invention, such a data communication session would be a Hypertext Transfer Protocol (HTTP) data session. The SSD 250 is operable to perform this session and serves up a "dashboard" 250, as illustrated at communication 220. Communication 221 illustrates the receipt of this "dashboard" 250 by the user 102, as well as the "dashboard" 250 enabling a "service" with CSG 130 in the path.

Communication 222 illustrates user 102 making a request on this "service," and the request is forwarded

by SSG 120 to the CSG 130.   As part of communication 222, the IP address of user 102 is provided.   When the CSG 130 receives communication 222, it attempts to locate the IP address received from user 102 stored in a mapping table 233 and associated with a user-ID.   If the CSG 130 is unable to locate a match of the IP address received from user 102 in memory, the CSG 130 issues a query at communication 224 to the SSG 120 that includes the IP address of user 102.   SSG 120 is operable to respond to the query at communication 226 from CSG 130 by returning the user-ID that corresponds to the IP address of user 102.   In a preferred embodiment of the present invention, the IP address of each SSG 120 is established along with the range of user IP addresses that can be allocated by that SSG 120.   The CSG 130 is thus able to determine the appropriate SSG 120 to query by determining which SSG 120 is allocated the address range that contains the IP address of the unknown user.

Once the CSG 130 determines the appropriate SSG 120 to query, the CSG 130 sends a message to the SSG 120 containing the IP address as is illustrated by communication 224.   In a preferred embodiment of the present invention, both the CSG 130 and SSG 120 communicate using the User Datagram Protocol (UDP) format.   The SSG 120 responds by sending a message containing the IP address and the associated user-ID to the CSG 130.   This is illustrated by communication 226. Upon receiving communication 226, the CSG 130 adds a new entry to a mapping table stored in memory.   The mapping table allows CSG 130 to recognize which incoming packets are associated with a given service.   In a preferred embodiment of the present invention, the mapping table

stores entries in a <source IP address, user-ID> format. CSG 130 is then able to retrieve a user profile associated with the IP address and user-ID in order to apply appropriate services specified therein.

FIGURE 3 shows data exchanges that occur when SSG 120 updates all interested CSGs 130. Updates may occur when the IP address of a user changes or an IP address is subsequently assigned to a different user that a user 102 has already been authenticated and queried by the CSG 130 in the above-described manner. It is likewise presumed that both the SSG 120 and CSG 130 have consistent information regarding the IP address and user-ID mapping. Communication 310 illustrates a user 102 opening an HTTP session with the SSD 250. User 102 subsequently logs off that network account and logs on to the network again with another account. SSD 250 notifies the SSG 120 by communication 320 that the user-ID for the data exchange session has changed. The SSG 120 responds by sending out a multicast UDP or other protocol update message to all CSGs 130 with which SSG 120 is communicating as shown by communication 330. The CSGs 130 will update the IP address and user-ID mapping stored in memory with the new IP address of user 102. Communication 340 illustrates the data traffic from user 102 that subsequently passes through the SSG 120 to CSG 130 now has the appropriate user-specific policies from the second account applied to it. Alternatively, SSG 120 may be set to send a message to CSG 130 on a periodic basis or for all new issues being routed to CSG 130 in order to update mapping table 223 without requiring CSG 130 to send a query for an update. CSG 130 ensures that the IP address and user-ID mappings are valid. A mapping may become invalid when

12

user 102 logs off network 100 or a SSG 120 failure occurs. Three techniques are employed to deal with validation of these mappings. First, upon SSG 120 detecting a network logoff event from user 102, SSG 120 issues a multicast message to all CSGs 130 with which the SSG 120 is communicating and communicates the user logoff event. In response, any CSG 130 with a mapping for the now logged-out user IP address removes the entry from its mapping table.

A second technique to ensure mapping validity is to define a minimum "keep alive" time interval for the mapping table entries stored in the memory of CSG 130. CSG 130 will issue a "keep alive" message to SSG 120 if the "keep alive" time interval expires and no other queries have succeeded. The CSG 130 executes the "keep alive" message by re-querying the SSG 120 with the IP address of one of the entries in the mapping table. If the mapping table stored in the memory of CSG 130 is empty (i.e., no users 102, 104 currently active) no "keep alive" message is sent. If CSG 130 does not receive a response from SSG 120 within a set period of time, for example twice the "keep alive" time interval, CSG 130 discards the entire mapping table from memory. In the event that SSG 120 resumes communication with CSG 130, CSG 130 issues queries to re-establish valid mappings. This technique is operable to resolve situations in which user logoff signals from SSG 120 are not properly communicated to CSG 130 due to network congestion or network failure. Similarly, periodic queries may be sent from CSG 130 to SSG 120 in order to validate mapping table 223.

   A third technique is employed when SSG 120 ceases to function and then resumes communication. Upon restart SSG 120 communicates a multicast "restart" signal to all CSGs 130 with which SSG 120 is communicating. Each CSG

5   130 responds to the "restart" signal by voiding the entire mapping table stored in memory and re-querying SSG 120. The mapping tables in CSGs 130 are destroyed and reconstructed upon the failure of SSG 120, because it would be possible for users 102, 104 to logon again,

10   possibly with different IP addresses, following the failure of SSG 120.

   FIGURE 4 shows an alternative simplified scheme of a Client Services Gateway (CSG) 130 in the communications network environment 100, including data exchanges that

15   will take place during a typical user login. User 102 opens a data communication session with SSG 120 and sends user-ID and password to the SSG 120 for authentication as illustrated by communication 210. In communication 212, SSG 120 queries authentication server 240.

20   Authentication server 240 responds with communication 214, thereby authenticating user 102 and allowing SSG 120 to bring up the user data session. User 102 then seeks to open a HTTP or other protocol communication session with communication 216. The SSG 120 handles this session

25   at communication 218 and serves up a SSD 250 as illustrated by communication 220. User 102 receives this SSD 250 and enables a "service," which has a CSG 130 in the path. User 102 makes a data request 222 on this "service," which is forwarded by the SSG 120 to CSG 130.

30   CSG 130 attempts to identify a user-ID for user 102 associated with the IP address received as part of the request, but during the first request from user 102 CSG

130 will be unable to do so. Therefore, CSG 130 issues a challenge to user 102 as opposed to the SSG 120 shown in FIGURE 2, at communication 410 to prompt user 102 to submit the user-ID and password. User 102 then submits the user-ID and password at communication 420. User 102 has now been required to submit a user-ID and password on two occasions: once when initiating a communication session with the SSG 120 and a second time when initiating a request through the CSG 130. When user 102 responds to the challenge from CSG 130, as illustrated by communication 420, CSG 130 communicates with authentication server 240 at communication 430. Authentication server 240 responds to communication 430 from CSG 130 with communication 440. After user 102 has been authenticated at the request of CSG 130, a data session may proceed.

Thus, it is apparent that there has been provided, in accordance with the present invention, a system, device, and method for communicating user identification information over a communications network that satisfies the advantages set forth above. Although the present invention has been described with respect to network interfaces referred to as Service Selection Gateways (SSGs) and Client Service Gateways (CSGs) the present invention may equally apply to other network interfaces to permit exchanges of such information as user-ID and Internet Protocol (IP) address mappings. Moreover, although discussed in terms of HTTP requests between a user and a CSG, the present invention may be equally implemented in any network that utilizes user identification information. Other examples may be readily ascertainable by those skilled in the art and may

be made herein without departing from the spirit and scope of the present invention as defined by the following claims.